I CLAIM:

1. A method for regulating the ability of a user to print on a printer, comprising the steps of:

receiving, at a printer, a print job from a user, where the print job includes a representation of a document and an aspect of the print job that is encrypted with a private key of the user;

verifying the user by decoding the aspect using a public key of the user, where the public key and the private key form a key pair; and

printing the document on the printer if the user is a verified user.

2. The method of claim 1, where the printer is located at a printing site and printing is contingent on re-verification of the user at the printing site.

3. The method of claim 2, where re-verification includes demonstrating possession of the private key by the user at the printing site.

4. The method of claim 3, where the private key is stored on a portable processor and possession is demonstrated with a locally-restricted optical signal.

5. The method of claim 1, where the aspect relates to content of the print job.

6. The method of claim 1, where the aspect, after encryption, is a digital signature.

7. The method of claim 1, where the public key is included in a digital certificate.

8. The method of claim 1, where the public key is included in the print job.

9. The method of claim 1, where the public key is obtained by the printer from a public key database.

10. The method of claim 1, where the public key is linked to an authorization table that permits the user to print on the printer.

11. The method of claim 1, where the print job is at least partially encrypted by the user with a public key of the printer.

12. A system for regulating the ability of a user to print on a printer, comprising:

a sending processor that includes a private key of a user, where the private key forms a key pair with a public key, the sending processor being adapted to encrypt an aspect of a print job using the private key and to send the print job and encrypted aspect over a network; and

a printer in communication with the sending processor, where the printer is adapted to receive the print job and encrypted aspect from the sending processor, to verify the user by decoding the encrypted aspect using the public key, and to print a document based on the print job if the user is a verified user.

13. The system of claim 12, where the printer is located at a printing site and the user is verified upon a demonstration that the user possesses the private key at the printing site.

14. The system of claim 12, further including a portable processor that stores the private key in memory and carries out the demonstration.

15. The system of claim 12, where the aspect relates to content of the print job.

16. The system of claim 12, where the aspect, after encryption, is a digital signature.

17. The system of claim 12, where the public key is included in a digital certificate.

18. The system of claim 12, where the public key is included in the print job.

19. The system of claim 12, where the public key is obtained by the printer from a public key database.

20. The system of claim 12, where the public key is linked to an authorization table that permits the user to print on the printer.

21. The system of claim 12, where the print job is at least partially encrypted with a public key of the printer.

22. A printer capable of regulating output of a print job from a user, comprising:

a printer in communication with a user and adapted to receive a print job that has an aspect encrypted with a private key of the user, to verify the user by decoding the aspect using a public key of the user that forms a key pair with the private key, and to output the print job based on verifying the user.

23. The printer of claim 22, where the printer is located at a printing site and is further adapted to re-verify the user by receiving a demonstration that the user possesses the private key at the printing site.

24. The printer of claim 23, where printer is adapted to receive the demonstration from a portable processor that stores the private key in memory.

25. The printer of claim 22, where the aspect relates to content of the print job.

26. The printer of claim 22, where the aspect, after encryption, is a digital signature.

27. The printer of claim 22, where the public key is included in a digital certificate.

28. The printer of claim 22, where the public key is included in the print job.

29. The printer of claim 22, where the public key is obtained by the printer from a public key database.